(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 209 934 A1

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
29.05.2002 Bulletin 2002/22

(51) Int Cl.7: H04Q 7/38, H04L 29/06

(21) Application number: 00125913.4

(22) Date of filing: 27.11.2000

(84) Designated Contracting States:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE TR
Designated Extension States:
AL LT LV MK RO SI

(71) Applicant: SIEMENS AKTIENGESELLSCHAFT
80333 München (DE)

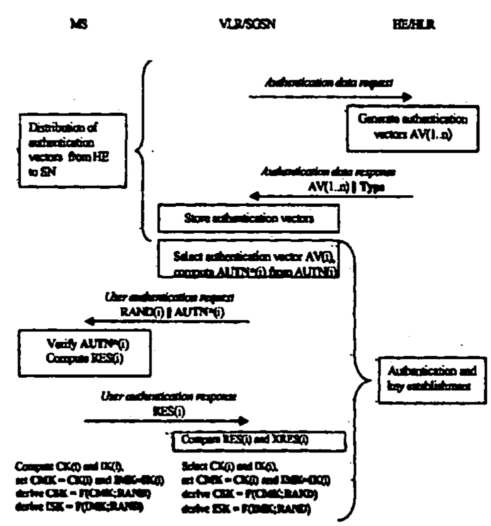
(72) Inventor: Horn, Guenther, Dr.
81541 München (DE)

(54) Method and apparatus to counter the rogue shell threat by means of local key derivation

(57) The invention concerns countering a rogue shell threat in a cellular mobile communication system by an apparatus or a method for authentication in a mobile communication system comprising a mobile communication network (VLR/SGSN/HLR/RNC...) and mobile stations (MS)

wherein the network provides a service to a mobile station (MS) after authentication of the mobile station wherein the mobile station (MS) comprises a portable module (USIM)
wherein the mobile station (MS) comprises a mobile equipment (ME) that is able to communicate with the network and that is able to communicate with the portable module (USIM) wherein the network sends random data (RAND) to the mobile station (MS)
wherein the network (AUC,SGSN) calculates response data (XRES (i)) and key data (CK,IK) at least from the random data (RAND) and/or from a key (K) stored in the network (AUC/HLR)
wherein the portable module (USIM) of the mobile station (MS) calculates response data (RES (i)) and key data (CK,IK) at least from the random data (RAND) and/or from a key (K) stored in the portable module (USIM)
wherein the portable module (USIM) stores the calculated key data (CK,IK)
wherein the portable module (USIM) transmits the response data (RES) to the mobile equipment (ME) which (ME) sends response data (RES) to the network
wherein the portable module calculates further key data (CSK,ISK) from random data (RAND) and/or from the calculated key data (CK,IK).

modified UMTS AKA supporting local key derivation:



The parameter "Type" indicates whether the USIM is old or new.
We have $AUTN^* = SQN \oplus AK \| AMF \| Enc_{CK}(MAC)$.
CMK and IMK are the cipher and integrity master keys, respectively.

Fig. 1

EP 1 209 934 A1

BEST AVAILABLE COPY

Printed by Jouve, 75001 PARIS (FR)

Description

[0001] A problem in communications systems in general is to make sure that only those parties authorised to use the resources of the communications system can actually use it. In this context, it is crucial to authenticate a communicating party, i.e. to corroborate the identity of the party by means of entity authentication. The corroborated identity may then be used in an access control mechanism (e.g. an access control list) to check which resources the party is authorised to use.

[0002] If the communication channel may be assumed to be secure (e.g. a fixed telephone line) then entity authentication may suffice to assure a party of another party's identity over the duration of a communication session. If, however, the communication channel may not be assumed to be secure (e.g. a mobile radio link or a link in the Internet) then an attacker could potentially "hijack" the channel, i.e. start to use the channel instead of the authorised party, without the other party noticing, after the completion of the entity authentication procedure.

[0003] Consequently, in the case of an insecure communication channel additional security measures are needed for continued assurance of a communicating party's identity during the session. Such additional security measures are the derivation of cryptographic session keys in conjunction with entity authentication and the use of these session keys in cryptographic algorithms to provide confidentiality and/or integrity protection of the communication channel. Confidentiality ensures that no unauthorised party can eavesdrop on the communication, and integrity ensures that no unauthorised party can modify the communication unnoticed. The communicating party's identity during the session is then continually assured by the use of the session keys. This holds under the assumption that only the authorised party can know the session keys.

[0004] This assumption depends on several factors, among them most prominently the strength and secure storage and execution of cryptographic algorithms and the secure storage of cryptographic keys.

[0005] The present invention applies to a situation where a communicating party, called the user, uses a communication device which consists of two components: a communication terminal and a user security module. The latter is a personal security device associated with the user which, among other functions, is used to store long-term cryptographic keys and store and execute cryptographic algorithms. To protect these cryptographic keys and algorithms, the user security module is typically implemented on a tamper-resistant hardware module. The communication terminal, on the other hand, enjoys only a considerably lower degree of protection against tampering. It is not permanently associated with a particular user. In the situation to which the invention applies the user security module is removable from the communication terminal and may be inserted in another communication terminal, making the second communication terminal the personal terminal of the user as long as the user security module remains inserted. Examples of such user security modules are the SIM module in GSM, the USIM module in UMTS and the WIM module in WAP. Examples of such communication terminals are the Mobile Equipment (ME) in GSM and UMTS and communication terminals supporting WAP.

[0006] In the situation to which the invention applies the cryptographic session keys used for confidentiality and/or integrity are derived jointly with entity authentication from one (or more) long-term cryptographic key (s) stored on the user security module. This session key derivation process can only be successfully performed by the user security module. The derived session keys are then transferred from the user security module to the communication terminal. (This transfer is motivated by performance considerations. It is more efficient to execute the confidentiality and/or integrity algorithms which use the session keys in the communication terminal.) When the user security module is removed from the communication terminal the latter is required to delete the session keys.

[0007] The problem which arises from the unavoidable transfer of the session keys to the communication terminal is the following: the continuous use of the session keys during the session is meant to continually ensure the communicating party's identity to the other party. But if the user security module is removed from the communication terminal and the latter is a rogue terminal not behaving according to the specifications the rogue terminal may decide to keep the session keys rather than delete them. If this occurs then the other party has no way of telling that the user is no longer associated with the communication terminal because the latter continues to use the session keys. An attacker in control of the rogue terminal may then use communication resources in the name of the user without the user knowing. This attack is also known as the rogue shell attack.

[0008] It is an object of the invention to avoid said rogue shell attack. The object of the invention is solved by the invention according to the independent claims. The invention can be used in any mobile communication network, especially in a cellular mobile communication network.

The invention applies to a situation where

a) it is costly to perform the entity authentication and key derivation procedure based on the long-term key in the user security module, and, therefore, it is advantageous to reduce the number of times this procedure has to be performed;

b) full backward compatibility with communication devices and other entities in the communication system which do not support the new feature described in the invention is desired.

[0009] Herein:

a) may apply when, in a mobile communications system, the entity authentication and key derivation procedure for a user roaming in a visited network involves signalling back to the home network.
b) may apply when a new feature to counter the rogue shell attack is introduced in an existing mobile communications system such as GSM, UMTS, ANSI IS-41 or a system defined by 3GPP2.

[0010] This invention presents a new way to counter the rogue shell attack in a situation where a) and, possibly in addition, b) hold.

[0011] Basically three approaches to deal with the rogue shell attack can be imagined:

1. Assume that most communication terminals are in fact personal devices of the user and that the user security module is relatively rarely removed and inserted in other communication terminals. If in such relatively rare cases rogue shell attacks occur one trusts that the attack can be detected and consequently countered by fraud control measures.
2. Perform the entity authentication and key derivation procedure with sufficient frequency so as to limit the lifetime of session keys and, consequently, limit the period during which fraud can be committed through unauthorised use of the session keys. The frequency must, of course, be sufficiently low so as not to incur unbearable costs.
3. Introduce a secondary authentication and key derivation procedure which is less costly to perform than the primary entity authentication and key derivation procedure. This secondary procedure is assumed, however, to not offer the same degree of security as the primary procedure for which reason the primary procedure still needs to be performed from time to time, but with reduced frequency.

[0012] In mobile communication networks, e.g. in GSM, a mixture of approaches 1 and 2 is applied. In UMTS Release'99, also a mixture of approaches 1 and 2 is expected to be applied.

[0013] The use of secondary authentication and key derivation procedures for different objects (to reduce the cost of the primary procedure) is known from prior art in different fields of technology, among them TETRA (Terrestrial Trunked Radio (TETRA), Voice plus Data (V+D): Part 7: Security; Edition 2f, November 1998), from DECT (ETS 300175-7, DECT Common Interface, Part 7: Security Features, European Telecommunications Standards Institute, 1992) and IS-41 (TIA/EIA, PN 2991: Cellular radio telecommunications intersystem operations IS-41 Rev. D; May 4 1995). They were not known or used in these systems, however, for the purpose of countering the rogue shell attack.

[0014] Recently, the use of secondary authentication and key derivation procedures to counter the rogue shell attack in 3GPP (UMTS) and 3GPP2 systems has been proposed in contributions to standards bodies, cf. [Lucent] (=Lucent Technologies Inc, M. Marcovici, S. Mizikovsky: Enhanced local authentication of a 3G mobile, TR45AHAG/00.09.12.15, Washington, DC, September 12, 2000) and [Qualcomm] (=F. Quick, J. Nasielski: Proposed security enhancement to AKA, TR45AHAG/2000.06.20., Ottawa, Canada, June 20, 2000-11-23). Both solutions modify, in different ways, key material which results from the primary key derivation procedure and use the modified key material as intermediate keys which are input to the secondary authentication and key derivation procedure.

Invention

[0015] Functional entities supporting the new feature described in the invention are called "new" here, and others not supporting it are called "old" here.

[0016] The principles followed by the invention are:

- Introduce a secondary authentication and key derivation procedure as in section 2.3 above
- Minimize the changes required to existing systems
- Re-use as much as possible protocol elements of the primary authentication and key derivation procedure
- Allow communication between old and new entities.

[0017] We consider two different situations:

- The general situation where a user with a communication device consisting of a communication terminal and a user security module communicates with a second party in a communications system;
- A specific situation where the communications system is a mobile communications system consisting of the following components:
    - a mobile station consisting of a mobile equipment and a user security module;
    - a base station system;
    - a visited network node;
    - a home network node.

[0018] In both situations, the communication terminal is not affected by the introduction of the new feature.

[0019] In the general situation, the following holds for the solution given in the invention:

- the second party has a means to determine whether the user security module is old or new; this means need not involve the user;
- the second party signals to a new user security module that it is new by applying a cryptographic function to a parameter in the first message and possibly further data in the primary authentication

and key derivation procedure in a specific way; the cryptographic function may be a hash function or an encryption function; except for the modification of the parameter in the first message, the information flow, message format and contents of the primary authentication and key derivation procedure may remain unchanged;

- when the user security module learns that the second party is new it decides to use a secondary authentication and key derivation procedure; the keys derived in the primary procedure (with the parameter in the first message modified) are then used as intermediate keys in the secondary procedure; the intermediate keys are not transferred to the communication terminal;
- when the user security module learns that the second party is old by detecting that the first message in the primary authentication and key derivation procedure was unmodified, it decides to use the keys derived in the primary procedure as session keys and transfers them to the communication terminal;

[0020] This procedure for new user security modules and new second parties to agree on the use of a secondary authentication and key derivation procedure and derive intermediate keys for use in this secondary procedure may apply to any secondary authentication and key derivation procedure.

- The invention also defines the use of a particular secondary procedure which best fits the principles of the solution stated above.
- This particular secondary authentication and key derivation procedure consists in a reduced version of the primary procedure where the information flow and all message formats are identical in the primary and secondary procedure, but where parts of the message content are substituted with pre-defined fixed values or other parameters, possibly derived by non-cryptographic means.

[0021] In the specific situation, in addition, the following holds for the solution given in the invention:

- the base station system is not affected by the introduction of the new feature;
- the second party is the visited network node;
- the means for the second party to determine whether the user security module is old or new is a particular parameter sent by the home network node; this parameter may be sent in response to a request by the visited network node for user authentication data;
- the only modification for a home network node required to support the new feature is the capability of sending the information on the type of user security module (old or new) in the particular parameter; the generation and format of user authentication data remains unchanged;
- the further data to which the cryptographic function is possibly applied when the second party signals to a new user security module that it is new may be part of the user authentication data, in particular a derived key contained in the user authentication data;
- the particular secondary authentication and key derivation procedure may involve sending part of the user authentication data containing a random challenge to the mobile station; the random challenge would then be input to the secondary key derivation procedure together with the intermediate key.

[0022] General advantages of the solution presented in this invention are:

- the cost involved in frequently running a primary entity authentication and key derivation procedure is reduced;
- it allows communication between old and new entities; full backward compatibility is provided;
- it minimizes the changes required to existing systems;
- it re-uses as much as possible protocol elements of the primary authentication and key derivation procedure;
- it provides a means to modify the primary authentication and key derivation procedure in a simple way so that it can be used as a secondary procedure;
- the communication terminal is not affected by the introduction of the new secondary authentication and key derivation procedure;
- in the specific situation to which this invention applies the mobile equipment and the base station system are not affected by the introduction of the new secondary authentication and key derivation procedure.

[0023] Advantages over the solution presented in [Qualcomm]:

- In the solution in [Qualcomm], for the purpose of backward compatibility it is required that the home network node generates different types of user authentication data in real-time, depending on the type of visited network node (old or new). This is unnecessary in the solution presented here.
- The solution in [Qualcomm] does not say anything about how the different entities learn whether they are old or new. The solution presented in this invention provides a mechanism for this.
- The solution in [Qualcomm] envisages that the use of the secondary authentication and key derivation procedure depends on support of the ME which the solution presented in this invention does not.

[0024] Advantages over the solution presented in [Lucent]:

- The part of the Lucent solution relying on the use of the anonymity key AK does not seem to work as described in [Lucent] as it seems to rest on the assumption that AK has 128 bits whereas it has only 48 bits in the discussed use in UMTS. Furthermore, the AK is not known to the visited network node.
- If the anonymity key AK cannot be used by the visited network node in the Lucent solution then different procedures to compute user authentication data are required to include a so-called LAK (intermediate key). In this case, or if AK has to be transferred from the home network node, a different format of the user authentication data is required and the interface between the visited and the home network node needs to be changed. This is not required in the solution presented here.
- There are two alternatives in the Lucent solution for the secondary authentication and key derivation procedure. Alternative 1 in the Lucent solution does not provide a security level comparable to the solution presented in this invention as the same key IK continues to be used between two runs of the primary authentication procedure. Alternative 2 in the Lucent solution affects both ME and base station system which the solution presented here does not.

[0025] The invention contains recognising that the information flows and message formats of the primary authentication and key derivation procedure could be maintained while only slightly modifying message contents to obtain the following additional features:

- signalling from a new visited network node to a new user security module that the former is new;
- providing a means for the user security module and the visited network node to derive intermediate keys;
- providing a secondary authentication and key derivation procedure;

[0026] It was further recognised that

- it is not necessary to modify the way the home network node generates user authentication data in order to support backward compatibility;

- the rogue shell threat can be countered without affecting the communication terminal / mobile equipment and the base station system at all;

- it is possible for the second party to signal to a new user security module that it is new by applying a cryptographic function to the first message and possibly further data in the primary authentication and key derivation procedure;

- the keys derived in the (modified) primary authentication and key derivation procedure can be used as intermediate keys in the secondary authentication and key derivation procedure;

- it is possible for the second party to signal to a new user security module that it is new by applying a cryptographic function to the first message and possibly further data in the primary authentication and key derivation procedure.

[0027] Further advantages of the invention appear from the claims and the following desciption of an example for carrying out the invention.

Figure 1 shows a primary entity authentication and key derivation procedure, combined with a secondary authentication and and key derivation procedure (local key derivation procedure)

Figure 2 shows a local key derivation procedure not combined with a primary entity authentication and key derivation procedure

[0028] In the example for carrying out the invention , the feasibility of the invention is demonstrated by applying it to the Universal Mobile Telecommunications System (UMTS), as standardised by 3GPP. For the security architecture, compare [SecArch=3G TS 33.102 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Security Architecture (Release 1999), version 3.6.0, October 2000].

[0029] In the description of the example for carrying out the invention , the specialised terminology known from UMTS is used because, otherwise, it may be more difficult to see the impact of the invention in the context of UMTS for somebody comparing the invention with the current UMTS specifications in [SecArch].

[0030] The terminology known from UMTS relates to the more general terminology used in the description of this invention above as follows:

[0031] Terminology used in the description of this invention → Terminology used in UMTS

visited network node → VLR/SGSN
home network node → HLR/AuC
base station system → RNC
communication device → mobile station (MS)
mobile equipment → mobile equipment (ME)
user security module → USIM
primary authentication and key derivation procedure → UMTS authentication and key agreement procedure (UMTS AKA)
secondary authentication and key derivation procedure → local key derivation procedure (not known from [SecArch])
intermediate key → master key (not known from

[SecArch])
authentication data → authentication vector (AV)
MAP is a protocol used in UMTS to carry authentication related information between the HLR/AuC and the VLR/SGSN
MAC stands for Message Authentication Code.

Detailed description of an example for carrying out the invention

[0032] There are four main elements to the solution presented in this invention:

- a mechanism to signal from the HLR/AuC to the VLR/SGSN that the USIM supports the local authentication procedure;
- a mechanism to signal from the VLR/SGSN to the USIM that the VLR/SGSN is running the local key derivation procedure: this is based on a specific modification by the VLR/SGSN of the user authentication request in a UMTS AKA which the USIM can recognise;
- a procedure to derive the cipher and integrity master keys CMK and IMK from the permanent key K: this is realised using the UMTS AKA;
- a procedure to derive the cipher and integrity session keys CSK and ISK from the cipher and integrity master keys CMK and IMK: this is realised using a stripped down version of the UMTSAKA.

[0033] These four elements are described in detail in the following. Their realisation is based on the following ideas:

Mechanism to signal from the HLR/AuC to the VLR/SGSN that the USIM supports the local key derivation procedure

A new HLR/AuC always includes a flag in its responses to Send Authentication Info MAP messages which indicates whether the USIM is new or old. Backwards compatibility is achieved by using well-known techniques commonly used to introduce extensions to MAP.
No further changes to the HLR/AuC are required. In particular, the process of generating authentication vectors is as specified in [SecArch].

Mechanism to signal from the VLR/SGSN to the USIM that the VLR/SGSN supports the local authentication procedure

New VLRs/SGSNs and new USIMs have a standardised encryption function *Enc* which operates on 64 bit blocks and has a 128 bit key.

[0034] When a new VLR/SGSN has received (together with an authentication vector) the indication from the HLR/AuC that the USIM is new, and it wants to use the local key derivation procedure then it sends a modified *User Authentication* Request message containing *(RAND, AUTN*)*, cf. [SecArch, section 6.3.3]. *AUTN** differs from *AUTN* in that the MAC-parameter is encrypted with *CK*, i.e.

$$AUTN^* = SQN \oplus AK \,||\, AMF \,||\, Enc_{CK}(MAC).$$

[0035] When a new USIM receives the parameters contained in the User Authentication Request message it proceeds as specified in [SecArch, section 6.3.3] to compute AK, MAC, RES, CK, IK. The USIM then compares the computed MAC with the received MAC.

- When the computed MAC and the received MAC match the USIM continues as specified in [SecArch, section 6.3.3], and no local key derivation procedure is used. In particular, CK and IK are transferred to the ME after successful authentication.
- When the computed MAC and the received MAC do not match the USIM encrypts the computed MAC with CK and compares it to the received MAC. When there is a match now, the USIM determines that the local key derivation procedure is run and proceeds as described further below.
- When there is still no match the USIM reports authentication failure to the ME.

[0036] Procedure to derive the integrity master key IMK from the permanent key K

- When the USIM has determined that the local key derivation procedure is run CK and IK are not transferred to the ME, but remain in the USIM. CK becomes the cipher master key CMK and IK becomes the integrity master key IMK. Cipher and integrity session keys CSK and ISK are derived from CMK and IMK according to the procedure described below. Then the authentication procedure is continued as specified in [SecArch].
- When the VLR/SGSN initiated a local key derivation procedure and receives the correct RES it proceeds to set CMK := CK and IMK:= IK.

[0037] Procedure to derive the cipher and integrity session keys CSK and ISK from the cipher and integrity master keys CMK and IMK (local key derivation procedure)
[0038] The purpose of the local key derivation is to prove the presence of the USIM by having the USIM derive new session keys.
[0039] Both new USIMs and new VLR/SGSNs possess a standardised key derivation function *F*.
[0040] Two cases need to be distinguished:

- Case A: derivation of cipher and integrity session keys for the first time after the establishment of cipher and integrity master keys;
- Case B: derivation of cipher and integrity session keys for the second or later times after the establishment of cipher and integrity master keys.

Case A:

[0041]

- the USIM and the VLR/SGSN compute CSK = F (CMK; RAND) and ISK = F(IMK; RAND) where RAND is the parameter contained in the User Authentication Request message and used to derive CMK and IMK according to the description above. F is a key derivation function , i.e. a cryptographic function with special properties suitable to derive cryptographic new keys from existing cryptographic keys.
- The USIM then transfers CSK and ISK to the ME. The VLR/SGSN transfers CSK and ISK to the RNC in the security mode set-up procedure. The ME and the RNC continue as specified for a run of the UMTS AKA in [SecArch].

Case B:

[0042]

- Whenever the VLR/SGSN determines that new *CSK* and *ISK* need to be derived and the lifetimes of *CMK* and *IMK* have not expired it sends a modified *User Authentication Request* message to the MS containing *(RAND, AUTN-L)*. *RAND* is a nonce generated by the VLR/SGSN and *AUTN-L* is equal to a pre-defined fixed value to signal to the USIM that a local key derivation procedure is run, and not a UMTS AKA.
- The ME cannot distinguish a run of the local key derivation procedure from a run of the UMTS AKA and behaves accordingly during the entire procedure.
- When the USIM detects that the received AUTN equals the fixed value AUTN-L and it determines that the lifetimes of CMK and IMK have not expired it returns a RES-L equal to a pre-defined fixed value and computes the session keys as CSK = F(CMK; RAND) and ISK = F(IMK; RAND).
- The USIM then transfers CSK and ISK to the ME.
- After receiving the correct response RES-L from the MS, the VLR/SGSN computes the session keys as CSK = F(CMK; RAND) and ISK = F(IMK; RAND) and transfers CSK and ISK to the RNC in the security mode set-up procedure.
- When the USIM determines that the lifetimes of CMK and IMK have expired it sends a RES equal to a different pre-defined fixed value back to the VLR/SGSN.
- When the lifetimes of CMK and IMK have expired the VLR/SGSN inititates a run of the UMTS AKA to establish new CMK and IMK.

Claims

1. Method for authentication in a mobile communication system comprising a mobile communication network
(VLR/SGSN/HLR/RNC...) and mobile stations (MS)
wherein the network provides a service to a mobile station (MS) after authentication of the mobile station
wherein the mobile station (MS) comprises a portable module (USIM)
wherein the mobile station (MS) comprises a mobile equipment (ME) that is able to communicate with the network and that is able to communicate with the portable module (USIM)
wherein the network sends random data (RAND) to the mobile station (MS)
wherein the network (AUC, SGSN) calculates response data (XRES(i)) and key data (CK, IK) at least from the random data (RAND) and/or from a key (K) stored in the network (AUC/HLR)
wherein the portable module (USIM) of the mobile station (MS) calculates response data (RES(i)) and key data (CK, IK) at least from the random data (RAND) and/or from a key (K) stored in the portable module (USIM)
wherein the portable module (USIM) stores the calculated key data (CK, IK)
wherein the portable module (USIM) transmits the response data (RES) to the mobile equipment (ME) which (ME) sends response data (RES) to the network
wherein the portable module calculates further key data (CSK, ISK) from random data (RAND) and/or from the calculated key data (CK, IK)
wherein the portable module transmits further key data (CSK, ISK) to the mobile equipment (ME) to enable communication between the mobile equipment (ME) and the network for providing a service to the mobile station (MS)
wherein the network calculates further key data (CSK, ISK) from random data (RAND) and/or from the calculated key data (CK, IK) to enable communication between the network for providing a service to the mobile station (MS) and the mobile equipment (ME).

Method according to claim 1, **characterized in that** the network compares at least the response data (RES) from the mobile equipment (ME) and the response data (XRES) calculated in the network during the authentication procedure.

2. Method according to any of the preceding claims, **characterized in that** for checking whether the portable module is connected to the mobile equipment a second authentication procedure is executed at a later time than the authentication procedure of claim 1, wherein the network sends random data (RAND) to the mobile station (MS) wherein the portable module calculates new further key data (CSK, ISK) from this random data (RAND) and/or from the stored key data (CK, IK) that was calculated in the authentication procedure of claim 1, wherein the network also calculates the new further key data (CSK, ISK) from this random data (RAND) and/or from the stored key data (CK, IK) that was calculated in the authentication procedure of claim 1, wherein the new further key data (CSK, ISK) is used for communication between the mobile equipment (ME) and the network (RNC/SGSN).

3. Method according to any of the preceding claims 2 or 3, **characterized in that** the network does not compare the response data (RES) from the mobile equipment (ME) and the response data (XRES) calculated in the network during the second authentication procedure.

4. Method according to any of the preceding claims, **characterized in that** in the mobile station only the portable module (USIM) stores the key data (CK, IK) and that the portable module (USIM) does not transfer the key data (CK, IK) to the mobile equipment (ME).

5. Method according to any of the preceding claims, **characterized in that** the portable module (USIM) transfers further key data (CSK, ISK) data calculated from key data (CK, IK) to the mobile equipment only if it receives command data (AUTN*(i)) from a network element indicating that the network is able to calculate the said further key data.

6. Method according to claim 6, **characterized in that** a network element (SGSN, AUC, VLR) only transfers command data (AUTN*(i)) to the portable card (USIM) if the network (HLR) has detected that the portable card (USIM) is able to calculate the said further key data (CSK, ISK).

7. Method according to any of the preceding claims, **characterized in that** the command data (AUTN*(i)) a network element (SGSN, AUC, VLR) transfers to the portable card is sent in the form of command data (AUTN(i)) requesting calculating key data (CK, IK) wherein the command data (AUTN*(i)) is understood by a portable module (USIM), that is able to calculate further key data (CSK, ISK), as a command to calculate further key data (CSK, ISK) wherein the command data (AUTN(i)) is understood by a portable module (USIM) that is not able to calculate further key data (CSK, ISK) as a command to calculate key data (CK, IK)

8. Method according to any of the preceding claims, **characterized in that** the network recognises that the portable module (USIM) is connected to the mobile equipment (ME) by sending challenge data to the mobile station requiring answer data, calculated using further key data, from the mobile station and comparing the response data transmitted from the mobile station with response data calculated in the network.

9. Method according to any of the preceding claims, **characterized in that** the portable module (USIM) transfers the key data (CK, IK) to the mobile equipment (ME) if the portable module (USIM) is not able to calculate further key data (CSK, ISK) and that the key data (CK, IK) is used for communication between the mobile equipment (ME) and the network.

10. Portable module (USIM, SIM) that is designed for use in a mobile equipment (ME) for mobile network (UMTS, CDMA, GSM)

- with a receiving device for receiving random data (RAND) and other data (AUTN*(i) etc) via the mobile equipment (ME)
- with a sending device for sending via the mobile equipment (ME) response data (RES) as a response to the random data (RAND)
- with a calculating device that is designed for calculating response data (RES= RES(i)) as a response to the received random data (RAND) and for calulating key data (IK, CK) from at least the random data (RAND) and/or a key (K) stored in the portable module (USIM)

wherein the portable module (USIM, SIM) further comprises a calculating device that is designed for calculating further key data (CSK, ISK) from at least the key data (CK, IK) and/or the random data (RAND).

11. Portable module according to claim 11, **characterized in that** the portable module (USIM, SIM) is designed for transmitting only the further key data (CSK, ISK) to the mobile equipment (ME), if command data (AUTN*(i)) received with random data (RAND) indi-

cates that the network is able to calculate the further key data (CSK, ISK).

12. Portable module according to any of the preceding claims 11-12,
characterized in that
the portable module (USIM, SIM) is designed for transmitting only key data (CK, IK) to the mobile equipment (ME), if command data (AUTN(i)) received with random data (RAND) indicates that the network is not able to calculate the further key data (CSK, ISK).

13. Portable module according to any of the preceding claims 11-13,
characterized in that
the portable module (USIM, SIM) is designed for executing a second authentication procedure,
receiving new random data (RAND) from the network via the mobile station (MS)
calculating new further key data (CSK, ISK) from this random data (RAND) and/or from the calculated key data (CK, IK)
transmitting new further key data (CSK, ISK) to the mobile equipment (ME) for enabling the mobile equipment (ME) to use new further key data (CSK, ISK) for communication between the mobile equipment (ME) and the network (RNC/SGSN).

14. Network element (AUC, VLR, SGSN) of a mobile communication network

- with a sending device for sending command data (AUTN*(i)) and random data (RAND) to a mobile station (MS) for starting an authentication procedure
- with a calculation device for calculating response data (XRES(i)) that the network element expects to receive as a response (RES) from the mobile station (MS)
- with a calculation device for calculating key data (IK, CK) from at least the random data and a key (K) stored in the network element (VLR, SGSN, AUC, HLR)
- with a calculation device for calculating further key data (ISK, CSK) from at least the random data (RAND) and/or the key data (IK, CK) stored in the network element (VLR, SGSN, AUC, HLR)

15. Network (SGSN, VLR, AUC) element according to claim 15,
characterized in that it comprises
means for receiving from a home location register information stating whether the portable card (USIM) is able to calculate the said further key data (CSK, ISK).

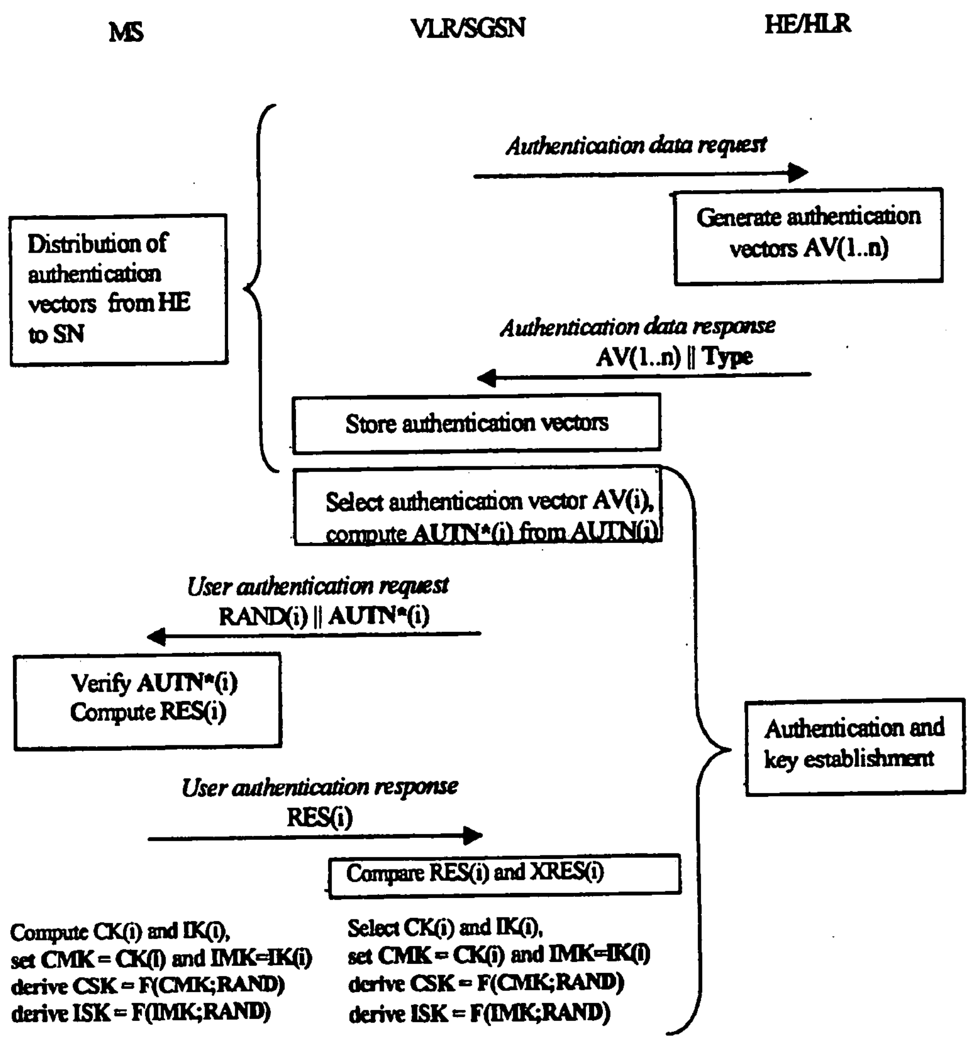
16. Network (SGSN, VLR, AUC) element according to claim 15 or 16,
characterized in that
it communicates with the mobile equipment using the key data (IK, CK) after detection that the portable card (USIM) is not able to calculate the said further key data (CSK, ISK).

17. Network (SGSN, VLR, AUC) element according to claim 15 or 16 or 17,
characterized in that
it communicates with the mobile equipment using the further key data (ISK, CSK) after detection that the portable card (USIM) is able to calculate the said further key data (CSK, ISK).

18. Network (SGSN, VLR, AUC) element according to claim 15 or 16 or 17 or 18,
characterized in that
it calculates command data (AUTN*(i)) after detection that the portable card (USIM) is able to calculate the said further key data (CSK, ISK) from command data (AUTN(i)) which it sends in case of detection that the portable card(USIM) is not able to calculate the said further key data (CSK, ISK).

19. Network (SGSN, VLR, AUC) element according to claim 15 or 16 or 17 or 18,
characterized in that
it calculates command data (AUTN*(i)) after detection that the portable card (USIM) is able to calculate the said further key data (CSK, ISK) from command data (AUTN(i)) which it sends in case of detection that the portable card (USIM) is not able to calculate the said further key data (CSK, ISK).

modified UMTS AKA supporting local key derivation:



The parameter "Type" indicates whether the USIM is old or new.
We have $AUTN^* = SQN \oplus AK \,||\, AMF \,||\, Enc_{CK}(MAC)$.
CMK and IMK are the cipher and integrity master keys, respectively.

Fig. 1

local key derivation procedure:

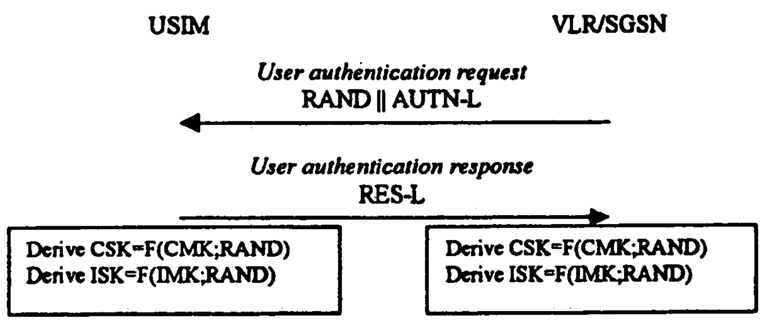


Fig. 2

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 00 12 5913

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.7)
A	MARCOVICI M ET AL: "Enhanced local authentication for a 3G mobile" TELECOMMUNICATIONS INDUSTRY ASSOCIATION TR 45 AHAG/TR45.2/00.08.15, 'Online! 15 August 2000 (2000-08-15), XP002177060 Retrieved from the Internet: <URL:http://ftp.tiaonline.org/TR-45/TR45MAIN/WORKING/2000nov/000830-05%20TR45%20TR45.2%20Report.pdf> 'retrieved on 2001-09-10! * the whole document *	1,11,15	H04Q7/38 H04L29/06
A	HORN G ET AL: "TOWARDS A UMTS SECURITY ARCHITECTURE" ITG-FACHBERICHTE, VDE VERLAG, BERLIN, DE, no. 157, 6 October 1999 (1999-10-06), pages 495-500, XP001023111 ISSN: 0932-6022 * figure 2 * * page 496 - page 498 *	1,11,15	

TECHNICAL FIELDS SEARCHED (Int.Cl.7)

H04Q
H04L

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
THE HAGUE	10 September 2001	Scalia, A

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)